IN THE CLAIMS

1-16 Cancelled

---

17. (Previously Presented) A method for establishing cryptographic communications, comprising the steps of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$0 \leq M \leq n-1$,

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and p_1, p_2, ..., P_k are distinct random prime numbers, C is a number representative of an encoded form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C, whereby

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

decoding said ciphertext word C to a receive message word M', said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1 -1)(p_2 -1) \ldots (p_k-1)),$$

said decoding step including the further steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} (\mathrm{mod}\ p_1),$$

$$M_2' \equiv C_2^{d_2} (\mathrm{mod}\ p_2),$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} (\mathrm{mod}\ p_k),$$

wherein

$$C_1 \equiv C (\mathrm{mod}\ p_1),$$

$$C_2 \equiv C (\mathrm{mod}\ p_2),$$

$$\vdots$$

$$C_k \equiv C (\mathrm{mod}\ p_k),$$

$$d_1 \equiv d (\mathrm{mod} (p_1 - 1)),$$

$$d_2 \equiv d (\mathrm{mod} (p_2 - 1)), \text{ and}$$

$$\vdots$$

$$d_k \equiv d(\bmod(p_k - 1)),$$

solving said sub-tasks to determine results $M_1', M_2', \ldots M_k'$, and

combining said results of said sub-tasks to produce said receive message word M', wherein $M' = M$.

18. (Original) A method as recited in claim 17 wherein said step of combining said results of said sub-tasks includes a step of performing a recursive combining process to produce said receive message word M'.

#1

19. (Original) A method as recited in claim 18 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + \left[(M_i' - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i \right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M' = Y_k, Y_1 = M_1', and\ w_i = \prod_{j<i} p_j .$$

20. (Original) A method as recited in claim 17 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said receive message word M'.

21. (Original) A method as recited in claim 20 wherein said summation process is performed in accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

22. (Previously Presented) A cryptographic communications system for establishing communications, comprising:

a communication medium;

encoding means coupled to said communication medium and adapted for transforming a transmit message word M to a ciphertext word C and for transmitting said

ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$, wherein n is a composite number of the form,

$n = p_1 \bullet p_2 \bullet \ldots \bullet p_k$

wherein k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, and wherein said ciphertext word C corresponds to a number representative of an enciphered form of said message word M and corresponds to

$C \equiv M^e (\bmod n)$,

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

H'

decoding means communicatively coupled with said communication medium for receiving said ciphertext word C via said medium, said decoding means being operative to perform a decryption process for transforming said ciphertext word C to a receive message word M', wherein M' corresponds to a number representative of a deciphered form of C, said decryption process using a decryption exponent d that is defined by

$d \equiv e^{-1} \bmod((p_1 - 1)(p_2 - 1)\ldots(p_k - 1))$,

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} (\bmod p_1),$$
$$M_2' \equiv C_2^{d_2} (\bmod p_2),$$
$$\vdots$$
$$M_k' \equiv C_k^{d_k} (\bmod p_k),$$

wherein

$$C_1 \equiv C (\bmod p_1),$$
$$C_2 \equiv C (\bmod p_2),$$
$$\vdots$$
$$C_k \equiv C (\bmod p_k),$$

$$d_1 \equiv d (\bmod (p_1 - 1)),$$
$$d_2 \equiv d (\bmod (p_2 - 1)), \text{ and}$$
$$\vdots$$
$$d_k \equiv d (\bmod (p_k - 1)),$$

solving said sub-tasks to determine results $M_1', M_2', \ldots M_k'$, and

combining said results of said sub-tasks to produce said receive message word M', wherein $M' = M$.

23. (Original) A cryptographic communications system as recited in claim 22 wherein said decoding means is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said receive message word M'.

24. (Original) A cryptographic communications system as recited in claim 23 wherein said decoding means is operative to perform said recursive combining process in accordance with

H'

$$Y_i \equiv Y_{i-1} + \left[(M_i' - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i\right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M' = Y_k, Y_1 = M_1', and\ w_i = \prod_{j<i} p_j.$$

25. (Original) A cryptographic communications system as recited in claim 22 wherein said decoding means is operative combine said results of said sub-tasks by performing a summation process to produce said receive message word M'.

26. (Original) A cryptographic communications system as recited in claim 25 wherein said decoding
means is operative to perform said summation process accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j.$$

27. (Previously Presented) A method for establishing cryptographic communications, comprising the step of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message, and

$$0 \leq M \leq n-1$$

n being a composite number formed from the product of $p_1 \cdot p_2 \bullet \ldots \bullet p_k$, wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, wherein said step of encoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} (\text{mod } p_1),$$
$$C_2 \equiv M_2^{e_2} (\text{mod } p_2),$$
$$\vdots$$
$$C_k \equiv M_k^{e_k} (\text{mod } p_k),$$

wherein

$$M_1 \equiv M (\text{mod } p_1),$$
$$M_2 \equiv M (\text{mod } p_2),$$
$$\vdots$$
$$M_k \equiv M (\text{mod } p_k),$$

$$e_1 \equiv e(\text{mod}(p_1 - 1)),$$
$$e_2 \equiv e(\text{mod}(p_2 - 1)), \text{ and}$$
$$\vdots$$
$$e_k \equiv e(\text{mod}(p_k - 1)),$$

wherein e is a number relatively prime to $(p_1\text{-}1)$, $(p_2\text{-}1)$, ..., and $(p_k\text{-}1)$, solving said sub-tasks to determine results $C_1, C_2, \ldots C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

28. (Original) A method as recited in claim 27 wherein said step of combining said results of said subtasks includes a step of performing a recursive combining process to produce said ciphertext word C.

29. (Original) A method as recited in claim 28 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + \left[(C_i - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i \right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$C = Y_k, Y_1 = C_1, and\ w_i = \prod_{j<i} p_j .$$

30. (Original) A method as recited in claim 27 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said ciphertext word C.

H

31. (Original) A method as recited in claim 30 wherein said summation process is performed in accordance with

$$C \equiv \sum_{i=1}^{k} C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

32. (Previously Presented) A cryptographic communications system for establishing communications, comprising:

a communication medium;

encoding means coupled to said communication medium and operative to transform a transmit message word M to a ciphertext word C, and to transmit said ciphertext word C on said medium, wherein .M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$ wherein k is an integer greater than 2 and p_1, p_2, ..., p_k, are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, said encoding means being operative to transform said transmit message word M to said ciphertext word C by performing an encoding process comprising the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} (\mathrm{mod}\ p_1),$$
$$C_2 \equiv M_2^{e_2} (\mathrm{mod}\ p_2),$$
$$\vdots$$
$$C_k \equiv M_k^{e_k} (\mathrm{mod}\ p_k),$$

wherein

$$M_1 \equiv M (\mathrm{mod}\ p_1),$$
$$M_2 \equiv M (\mathrm{mod}\ p_2),$$
$$\vdots$$
$$M_k \equiv M (\mathrm{mod}\ p_k),$$
$$e_1 \equiv e(\mathrm{mod}(p_1 - 1)),$$
$$e_2 \equiv e(\mathrm{mod}(p_2 - 1)), \text{ and}$$
$$\vdots$$
$$e_k \equiv e(\mathrm{mod}(p_k - 1)),$$

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1), solving said sub-tasks to determine results C_1, C_2, ... C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

33. (Original) A cryptographic communications system as recited in claim 32 wherein said encoding means is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said ciphertext word C.

34. (Original) A cryptographic communications system as recited in claim 33 wherein said encoding means is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + \left[(C_i - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i\right] \bullet w_i \bmod n,$$

wherein $2 \le i \le k$, and

$$C = Y_k, Y_1 = C_1, and\ w_i = \prod_{j<i} p_j.$$

35. (Original) A cryptographic communications system as recited in claim 32 wherein said encoding means is operative to combine said results of said sub-tasks by performing a summation process to produce said message word C.

36. (Original) A cryptographic communications system as recited in claim 35 wherein said encoding
means is operative to perform said summation process in accordance with

$$C \equiv \sum_{i=1}^{k} C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

#1

37. (Previously Presented) A method for establishing cryptographic communications, comprising the steps of:

decoding a ciphertext word C to a message word M, wherein M corresponds to a number representative of a message and wherein

$$0 \leq M \leq n-1$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, C is a number representative of an encoded form of message word M that is encoded by transforming said message word M to said ciphertext word C whereby

$C \equiv M^e (\text{mod } n)$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1);

said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1 - 1)(p_2 - 1) \ldots (p_k - 1)),$$

wherein said step of decoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$$M_1 \equiv C_1^{d_1} (\text{mod } p_1),$$

$$M_2 \equiv C_2^{d_2} (\text{mod } p_2),$$

$$\vdots$$

$$M_k \equiv C_k^{d_k} (\text{mod } p_k),$$

wherein

$$C_1 \equiv C(\bmod\, p_1),$$
$$C_2 \equiv C(\bmod\, p_2),$$
$$\vdots$$
$$C_k \equiv C(\bmod\, p_k),$$

$$d_1 \equiv d(\bmod(p_1 - 1)),$$
$$d_2 \equiv d(\bmod(p_2 - 1)), \text{ and}$$
$$\vdots$$
$$d_k \equiv d(\bmod(p_k - 1)),$$

solving said sub-tasks to determine results M_1, M_2,... M_k, and combining said results of said sub-tasks to produce said message word M.

38. (Original) A method as recited in claim 37 wherein said step of combining said results of said sub-tasks includes a step of performing a recursive combining process to produce said message word M.

39. (Original) A method as recited in claim 38 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + \left[(M_i - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i\right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M' = Y_k, Y_1 = M_1', and\ w_i = \prod_{j<i} p_j .$$

40. (Original) A method as recited in claim 37 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said message word M.

41. (Original) A method as recited in claim 40 wherein said summation process is performed in accordance with

$$M \equiv \sum_{i=1}^{k} M_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

42. (Previously Presented) A cryptographic communications system for establishing communications, comprising:

a communication medium;

decoding means communicatively coupled with said communication medium for receiving a ciphertext word C via said medium, and being operative to transform said ciphertext word C to a receive message word M', wherein a message M corresponds to a number representative of a message and wherein,

$$0 \leq M \leq n-1$$

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, and wherein said ciphertext word C is a number representative of an encoded form of said message word M that is encoded by transforming M to said ciphertext word C whereby,

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1);

said decoding means being operative to perform a decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1)\ldots(p_k-1)),$$

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with,

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C(\text{mod } p_1),$$
$$C_2 \equiv C(\text{mod } p_2),$$
$$\vdots$$
$$C_k \equiv C(\text{mod } p_k),$$

$$d_1 \equiv d(\text{mod}(p_1 - 1)),$$
$$d_2 \equiv d(\text{mod}(p_2 - 1)), \text{ and}$$
$$\vdots$$
$$d_k \equiv d(\text{mod}(p_k - 1)),$$

H!

solving said sub-tasks to determine results $M_1', M_2', \ldots M_k'$, and

combining said results of said sub-tasks to produce said receive message word M', wherein $M' = M$.

43. (Original) A cryptographic communications system as recited in claim 42 wherein said decoding means is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said receive message word M'.

44. (Original) A cryptographic communications system as recited in claim 41 wherein said decoding means is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + \left[(M_i' - Y_{i-1})(w_i^{-1} \text{ mod } p_i) \text{ mod } p_i\right] \bullet w_i \text{ mod } n,$$

wherein $2 \leq i \leq k$, and

$$M = Y_k, Y_1 = M_1', \textit{and } w_i = \prod_{j<i} p_j .$$

45. (Original) A cryptographic communications system as recited in claim 42 wherein said decoding means is operative to combine said results of said sub-tasks by performing a summation process to produce said receive message word M'.

46. (Original) A cryptographic communications system as recited in claim 45 wherein said decoding

means is operative to perform said summation process in accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

47. (Previously Presented) A method for generating a digital signature, comprising the step of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message, and

$$0 \leq M \leq n-1,$$

n being a composite number formed from the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, wherein k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of message word M, wherein

$C \equiv M^d (\bmod n)$, and

wherein said step of signing includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{d_1} (\bmod p_1),$$

$$C_2 \equiv M_2^{d_2} (\bmod p_2),$$

$$\vdots$$

$$C_k \equiv M_k^{d_k} (\bmod p_k),$$

wherein

$$M_1 \equiv M (\bmod p_1),$$

$$M_2 \equiv M (\bmod p_2),$$

$$\vdots$$

$$M_k \equiv M (\bmod p_k),$$

$$d_1 \equiv d(\bmod(p_1 - 1)),$$

$d_2 \equiv d(\bmod(p_2 - 1))$, and

$$\vdots$$

$$d_k \equiv d(\bmod(p_k - 1)),$$

where d id defined by

$d \equiv e^{-1} \bmod((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1), solving said sub-tasks to determine results C_1, C_2, ... C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

48. (Original) A method as recited in claim 47 wherein said step of combining said results of said sub-asks includes a step of performing a recursive combining process to produce said ciphertext word C.

49. (Original) A method as recited in claim 48 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + \left[(C_i - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i\right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$C = Y_k, Y_1 = C_1, and\ w_i = \prod_{j<i} p_j .$$

#'

50. (Original) A method as recited in claim 47 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said signed ciphertext word C.

51. (Original) A method as recited in claim 50 wherein said summation process is performed in accordance with

$$C \equiv \sum_{i=1}^{k} C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

52. (Previously Presented) A digital signature generation system, comprising:

a communication medium;

digital signature generating means coupled to said communication medium and operative to transform a transmit message word M to a signed ciphertext word C, and to transmit said

signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$$0 \leq M \leq n-1,$$

n being a composite number formed from the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k wherein k is an integer greater than 2 and p_1, p_2, ..., p_k, are distinct random prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of said message word M, wherein

$$C \equiv M^d (\bmod n),$$

said digital signature generating means being operative to transform said transmit message word M to said signed ciphertext word C by performing a digital signature generating process comprising the steps of,

#1

defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{d_1} (\bmod p_1),$$

$$C_2 \equiv M_2^{d_2} (\bmod p_2),$$

$$\vdots$$

$$C_k \equiv M_k^{d_k} (\bmod p_k),$$

wherein

$$M_1 \equiv M (\bmod p_1),$$

$$M_2 \equiv M (\bmod p_2),$$

$$\vdots$$

$$M_k \equiv M (\bmod p_k),$$

$$d_1 \equiv d (\bmod (p_1 - 1)),$$

$$d_2 \equiv d (\bmod (p_2 - 1)), \text{ and}$$

$$\vdots$$

$$d_k \equiv d (\bmod (p_k - 1)),$$

where d id defined by

$$d \equiv e^{-1} \bmod ((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1)), \text{ and}$$

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1), solving said sub-tasks to determine results C_1, C_2, ... C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

53. (Original) A digital signature generation system as recited in claim 52 wherein said signature generating means is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said signed ciphertext word C.

54. (Original) A digital signature generation system as recited in claim 53 wherein said digital signature generating means is operative to perform said recursive combining process in accordance with $Y_i \equiv Y_{i-1} + \left[(M_i' - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i\right] \bullet w_i \bmod n,$

wherein $2 \leq i \leq k$, and

$C = Y_k, Y_1 = C_1, and\ w_i = \prod_{j<i} p_j$.

55. (Original) A digital signature generation system as recited in claim 52 wherein said signature generating means is operative to combine said results of said sub-tasks by performing a summation process to produce said signed message word C.

56. (Original) A digital signature system as recited in claim 55 wherein said signature generating means
is operative to perform said summation process in accordance with

$$C \equiv \sum_{i=1}^{k} C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

57. (Previously Presented) A digital signature process, comprising the steps of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$0 \leq M \leq n-1$

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, C is a number representative of a signed form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C whereby,

$C = M^d \pmod{n}$,

wherein d is defined by

$d \equiv e^{-1} \bmod((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

verifying said ciphertext word C to a receive message word M' by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} (\bmod p_1),$$

$$M_2' \equiv C_2^{e_2} (\bmod p_2),$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} (\bmod p_k),$$

wherein

$$C_1 \equiv C(\bmod p_1),$$

$$C_2 \equiv C(\bmod p_2),$$

$$\vdots$$

$$C_k \equiv C(\bmod p_k),$$

$$e_1 \equiv e(\bmod(p_1 - 1)),$$

$$e_2 \equiv e(\bmod(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$e_k \equiv e(\bmod(p_k - 1)),$$

solving said sub-tasks to determine results $M_1', M_2', \ldots M_k'$, and

combining said results of said sub-tasks to produce said receive message word M', wherein $M' = M$.

58. (Original) A digital signature process as recited in claim 57 wherein said step of combining said results of said sub-tasks includes a step of performing a recursive combining process to produce said receive message word M'.

59. (Original) A digital signature process as recited in claim 58 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + \left[(M_i' - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i\right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M' = Y_k, Y_1 = M_1', \textit{and } w_i = \prod_{j<i} p_j .$$

60. (Original) A digital signature process as recited in claim 58 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said receive message word M'.

61. (Original) A digital signature process as recited in claim 60 wherein said summation process is performed in accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

62. (Previously Presented) A digital signature system, comprising:

a communication medium;

digital signature generating means coupled to said communication medium and adapted for transforming a message word M to a signed ciphertext word C and for transmitting said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$, wherein n is a composite number of the form

$n=p_1 \bullet p_2 \bullet \ldots \bullet p_k$,

wherein k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, and wherein said signed ciphertext word C corresponds to a number representative of a signed form of said message word M and corresponds to

$C \equiv M^d \pmod{n}$,

wherein d is defined by

$d \equiv e^{-1} \bmod((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (P_2-1), ..., and (p_k-1); and

digital signature verification means communicatively coupled with said communication medium for receiving said signed ciphertext word C via said medium, and being operative to verify said signed ciphertext word C by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} (\text{mod } p_1),$$

$$M_2' \equiv C_2^{e_2} (\text{mod } p_2),$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} (\text{mod } p_k),$$

wherein

$$C_1 \equiv C(\text{mod } p_1),$$

$$C_2 \equiv C(\text{mod } p_2),$$

$$\vdots$$

$$C_k \equiv C(\text{mod } p_k),$$

$$e_1 \equiv e(\text{mod}(p_1 - 1)),$$

$$e_2 \equiv e(\text{mod}(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$e_k \equiv e(\text{mod}(p_k - 1)),$$

solving said sub-tasks to determine results $M_1', M_2', ...M_k'$, and

combining said results of said sub-tasks to produce said receive message word M', wherein $M' = M$.

63. (Original) A digital signature system as recited in claim 62 wherein said decoding means is operative to combine said results of saïd sub-tasks by performing a recursive combining process to produce said receive message word M'.

64. (Original) A digital signature system as recited in claim 63 wherein said decoding means is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + \left[(M_i' - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i\right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M' = Y_k, Y_1 = M_1', \textit{and } w_i = \prod_{j<i} p_j .$$

65. (Original) A digital signature system as recited in claim 62 wherein said decoding means is operative combine said results of said sub-tasks by performing a summation process to produce said receive message word M'.

66. (Original) A digital signature system as recited in claim 65 wherein said decoding means is operative to perform said summation process accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

67-72 Cancelled

73. (Original) A method as recited in claim 17 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

74. (Original) A method as recited in claim 17 wherein each of said distinct random prime number has the same number of bits.

75. (Original) A cryptographic communications system as recited in claim 22 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

76. (Original) A cryptographic communications system as recited in claim 22 wherein each of said distinct random prime number has the same number of bits.

77. (Original) A method as recited in claim 27 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

78. (Original) A method as recited in claim 27 wherein each of said distinct random prime number has the same number of bits.

79. (Original) A cryptographic communications system as recited in claim 32 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

80. (Original) A cryptographic communications system as recited in claim 32 wherein each of said distinct random prime number has the same number of bits.

81. (Original) A method as recited in claim 37 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

82. (Original) A method as recited in claim 37 wherein each of said distinct random prime number has the same number of bits.

83. (Original) A cryptographic communications system as recited in claim 42 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

84. (Original) A cryptographic communications system as recited in claim 42 wherein each of said distinct random prime number has the same number of bits.

85. (Original) A method as recited in claim 47 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

86. (Original) A method as recited in claim 47 wherein each of said distinct random prime number has the same number of bits.

87. (Original) A digital signature generation system as recited in claim 52 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

88. (Original) A digital signature generation system as recited in claim 52 wherein each of said distinct
random prime number has the same number of bits.

89. (Original) A digital signature process as recited in claim 57 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

90. (Original) A digital signature process as recited in claim 57 wherein each of said distinct random prime number has the same number of bits.

91. (Original) A digital signature system as recited in claim 62 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

92. (Original) A digital signature system as recited in claim 62 wherein each of said distinct random prime number has the same number of bits.

93. (Previously Presented) A method as recited in claim 17 wherein the plurality of k sub-tasks are performed in parallel.

94. (Previously Presented) A method as recited in claim 93 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

95. (Previously Presented) A cryptographic communications system as recited in claim 22 wherein the plurality of k sub-tasks are performed in parallel.

96. (Previously Presented) A cryptographic communications system as recited in claim 95 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

97. (Previously Presented) A method as recited in claim 27 wherein the plurality of k sub-tasks are performed in parallel.

98. (Previously Presented) A method as recited in claim 97 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

99. (Previously Presented) A cryptographic communications system as recited in claim 32 wherein the plurality of k sub-tasks are performed in parallel.

100. (Previously Presented) A cryptographic communications system as recited in claim 99 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

101. (Previously Presented) A method as recited in claim 37 wherein the plurality of k sub-tasks are performed in parallel.

102. (Previously Presented) A method as recited in claim 101 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

103. (Previously Presented) A cryptographic communications system as recited in claim 42 wherein the plurality of k sub-tasks are performed in parallel.

104. (Previously Presented) A cryptographic communications system as recited in claim 103 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

105. (Previously Presented) A method as recited in claim 47 wherein the plurality of k sub-tasks are performed in parallel.

106. (Previously Presented) A method as recited in claim 105 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

107. (Previously Presented) A digital signature generation system as recited in claim 52 wherein the plurality of k sub-tasks are performed in parallel.

108. (Previously Presented) A digital signature generation system as recited in claim 107 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

109. (Previously Presented) A digital signature process as recited in claim 57 wherein the plurality of k sub-tasks are performed in parallel.

110. (Previously Presented) A digital signature process as recited in claim 109 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

111. (Previously Presented) A digital signature system as recited in claim 62 wherein the plurality of k sub-tasks are performed in parallel.

112. (Previously Presented) A digital signature system as recited in claim 111 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

113. (New) A method for establishing cryptographic communications, comprising the steps of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$0 \leq M \leq n-1$,

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2 and $p_1, p_2, \ldots, P_k$ are distinct random prime numbers, C is a number representative of an encoded form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C, whereby

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

decoding said ciphertext word C to a receive message word M', said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1 -1)(p_2 -1) \ldots (p_k-1)),$$

said decoding step including the further steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} (\bmod p_1),$$

$$M_2' \equiv C_2^{d_2} (\bmod p_2),$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} (\bmod p_k),$$

wherein

$$C_1 \equiv C (\bmod p_1),$$

$$C_2 \equiv C (\bmod p_2),$$

$$\vdots$$

$$C_k \equiv C (\bmod p_k),$$

$$d_1 \equiv d(\bmod(p_1 - 1)),$$

$$d_2 \equiv d(\bmod(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$d_k \equiv d(\bmod(p_k - 1)),$$

solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results $M_1', M_2', \ldots M_k'$, and

combining said results of said sub-tasks to produce said receive message word M', wherein $M' = M$.

114. (New) A cryptographic communications system for establishing communications, comprising:

a communication medium;

encoding means coupled to said communication medium and adapted for transforming a transmit message word M to a ciphertext word C and for transmitting said

41

ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$, wherein n is a composite number of the form,

$n = p_1 \bullet p_2 \bullet \ldots \bullet p_k$

wherein k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, and wherein said ciphertext word C corresponds to a number representative of an enciphered form of said message word M and corresponds to

$C \equiv M^e (\bmod n)$,

wherein e is a number relatively prime to $(p_1\text{-}1)$, $(p_2\text{-}1)$, ..., and $(p_k\text{-}1)$; and

decoding means communicatively coupled with said communication medium for receiving said ciphertext word C via said medium, said decoding means being operative to perform a decryption process for transforming said ciphertext word C to a receive message word M', wherein M' corresponds to a number representative of a deciphered form of C, said decryption process using a decryption exponent d that is defined by

11'

$d \equiv e^{-1} \bmod((p_1 - 1)(p_2 - 1)\ldots(p_k - 1))$,

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} (\bmod p_1),$$
$$M_2' \equiv C_2^{d_2} (\bmod p_2),$$
$$\vdots$$
$$M_k' \equiv C_k^{d_k} (\bmod p_k),$$

wherein

$$C_1 \equiv C (\bmod p_1),$$
$$C_2 \equiv C (\bmod p_2),$$
$$\vdots$$
$$C_k \equiv C (\bmod p_k),$$

$$d_1 \equiv d (\bmod (p_1 - 1)),$$
$$d_2 \equiv d (\bmod (p_2 - 1)), \text{ and}$$
$$\vdots$$
$$d_k \equiv d (\bmod (p_k - 1)),$$

solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results $M_1', M_2', \ldots M_k'$, and

combining said results of said sub-tasks to produce said receive message word M', wherein $M' = M$.

115. (New) A method for establishing cryptographic communications, comprising the step of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message, and

$$0 \leq M \leq n-1$$

n being a composite number formed from the product of $p_1 \cdot p_2 \bullet \ldots \bullet p_k$, wherein k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, wherein said step of encoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} (\bmod\, p_1),$$
$$C_2 \equiv M_2^{e_2} (\bmod\, p_2),$$
$$\vdots$$
$$C_k \equiv M_k^{e_k} (\bmod\, p_k),$$

wherein

$$M_1 \equiv M (\bmod\, p_1),$$
$$M_2 \equiv M (\bmod\, p_2),$$
$$\vdots$$
$$M_k \equiv M (\bmod\, p_k),$$

$$e_1 \equiv e(\bmod (p_1 - 1)),$$
$$e_2 \equiv e(\bmod (p_2 - 1)), \text{ and}$$
$$\vdots$$
$$e_k \equiv e(\bmod (p_k - 1)),$$

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1), solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results C_1, C_2, ... C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

116. (New) A cryptographic communications system for establishing communications, comprising:

a communication medium;

encoding means coupled to said communication medium and operative to transform a transmit message word M to a ciphertext word C, and to transmit said ciphertext word C on said medium, wherein .M corresponds to a number representative of a message, and

$$0 \leq M \leq n-1,$$

n being a composite number formed from the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$ wherein k is an integer greater than 2 and p_1, p_2, ..., p_k, are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, said encoding means being operative to transform said transmit message word M to said ciphertext word C by performing an encoding process comprising the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} (\text{mod } p_1),$$

$$C_2 \equiv M_2^{e_2} (\text{mod } p_2),$$

$$\vdots$$

$$C_k \equiv M_k^{e_k} (\text{mod } p_k),$$

wherein

$$M_1 \equiv M (\text{mod } p_1),$$

$$M_2 \equiv M (\text{mod } p_2),$$

$$\vdots$$

$$M_k \equiv M (\text{mod } p_k),$$

$$e_1 \equiv e(\text{mod}(p_1 - 1)),$$

$$e_2 \equiv e(\text{mod}(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$e_k \equiv e(\text{mod}(p_k - 1)),$$

wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1), solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results C_1, C_2, ... C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

117. (New) A method for establishing cryptographic communications, comprising the steps of:

decoding a ciphertext word C to a message word M, wherein M corresponds to a number representative of a message and wherein

$$0 \le M \le n-1$$

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, C is a number representative of an encoded form of message word M that is encoded by transforming said message word M to said ciphertext word C whereby

$$C \equiv M^e (\bmod n),$$

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1);

said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1)\ldots(p_k-1)),$$

wherein said step of decoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$$M_1 \equiv C_1^{d_1} (\bmod p_1),$$

$$M_2 \equiv C_2^{d_2} (\bmod p_2),$$

$$\vdots$$

$$M_k \equiv C_k^{d_k} (\bmod p_k),$$

wherein

$$C_1 \equiv C (\bmod p_1),$$

$$C_2 \equiv C (\bmod p_2),$$

$$\vdots$$

$$C_k \equiv C (\bmod p_k),$$

$$d_1 \equiv d (\bmod (p_1-1)),$$

$$d_2 \equiv d(\bmod(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$d_k \equiv d(\bmod(p_k - 1)),$$

solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results M_1, M_2,... M_k, and

combining said results of said sub-tasks to produce said message word M.

118. (New) A cryptographic communications system for establishing communications, comprising:

41

a communication medium;

decoding means communicatively coupled with said communication medium for receiving a ciphertext word C via said medium, and being operative to transform said ciphertext word C to a receive message word M', wherein a message M corresponds to a number representative of a message and wherein,

$$0 \le M \le n-1$$

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, and wherein said ciphertext word C is a number representative of an encoded form of said message word M that is encoded by transforming M to said ciphertext word C whereby,

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1);

said decoding means being operative to perform a decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod((p_1 - 1)(p_2 - 1)\ldots(p_k - 1)),$$

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with,

$$M_1' \equiv C_1^{d_1} (\bmod\ p_1),$$

$$M_2' \equiv C_2^{d_2} (\bmod\ p_2),$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} (\bmod\ p_k),$$

wherein

$$C_1 \equiv C(\text{mod } p_1),$$
$$C_2 \equiv C(\text{mod } p_2),$$
$$\vdots$$
$$C_k \equiv C(\text{mod } p_k),$$

$$d_1 \equiv d(\text{mod}(p_1 - 1)),$$
$$d_2 \equiv d(\text{mod}(p_2 - 1)), \text{ and}$$
$$\vdots$$
$$d_k \equiv d(\text{mod}(p_k - 1)),$$

H1

solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results $M_1', M_2', \ldots M_k'$, and

combining said results of said sub-tasks to produce said receive message word M', wherein $M' = M$.

119. (New) A method for generating a digital signature, comprising the step of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, wherein k is an integer greater than 2 and p_1, p_2, …, p_k are distinct random prime numbers, and wherein the signed cipher text word C is a number representative of a signed form of message word M, wherein

$C \equiv M^d (\text{mod}\, n)$, and

wherein said step of signing includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{d_1} (\text{mod } p_1),$$
$$C_2 \equiv M_2^{d_2} (\text{mod } p_2),$$
$$\vdots$$
$$C_k \equiv M_k^{d_k} (\text{mod } p_k),$$

wherein

$$M_1 \equiv M (\text{mod } p_1),$$

$$M_2 \equiv M(\bmod p_2),$$

$$\vdots$$

$$M_k \equiv M(\bmod p_k),$$

$$d_1 \equiv d(\bmod(p_1 - 1)),$$

$$d_2 \equiv d(\bmod(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$d_k \equiv d(\bmod(p_k - 1)),$$

H')

where d id defined by

$d \equiv e^{-1} \bmod((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1), solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results C_1, C_2, ... C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

120. (New) A digital signature generation system, comprising:

a communication medium;

digital signature generating means coupled to said communication medium and operative to transform a transmit message word M to a signed ciphertext word C, and to transmit said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n - 1$,

n being a composite number formed from the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k wherein k is an integer greater than 2 and p_1, p_2, ..., p_k, are distinct random prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of said message word M, wherein

$C \equiv M^d (\bmod n)$,

said digital signature generating means being operative to transform said transmit message word M to said signed ciphertext word C by performing a digital signature generating process comprising the steps of,

defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{d_1} (\bmod p_1),$$

$$C_2 \equiv M_2^{d_2} (\text{mod } p_2),$$
$$\vdots$$
$$C_k \equiv M_k^{d_k} (\text{mod } p_k),$$

wherein

$$M_1 \equiv M (\text{mod } p_1),$$
$$M_2 \equiv M (\text{mod } p_2),$$
$$\vdots$$
$$M_k \equiv M (\text{mod } p_k),$$

$$d_1 \equiv d(\text{mod}(p_1 - 1)),$$
$$d_2 \equiv d(\text{mod}(p_2 - 1)), \text{ and}$$
$$\vdots$$
$$d_k \equiv d(\text{mod}(p_k - 1)),$$

H'

where d id defined by

$d \equiv e^{-1} \text{mod}((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), …, and (p_k-1), solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results C_1, C_2, … C_k, and

combining said results of said sub-tasks to produce said ciphertext word C.

121. (New) A digital signature process, comprising the steps of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$0 \leq M \leq n-1$

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2 and p_1, p_2, …, p_k are distinct random prime numbers, C is a number representative of a signed form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C whereby,

$C = M^d$ (mod n),

wherein d is defined by

$d \equiv e^{-1} \text{mod}((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to (p_1-1), (p_2-1), ..., and (p_k-1); and

verifying said ciphertext word C to a receive message word M' by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} (\text{mod } p_1),$$

$$M_2' \equiv C_2^{e_2} (\text{mod } p_2),$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} (\text{mod } p_k),$$

wherein

$$C_1 \equiv C(\text{mod } p_1),$$

$$C_2 \equiv C(\text{mod } p_2),$$

$$\vdots$$

$$C_k \equiv C(\text{mod } p_k),$$

$$e_1 \equiv e(\text{mod}(p_1 - 1)),$$

$$e_2 \equiv e(\text{mod}(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$e_k \equiv e(\text{mod}(p_k - 1)),$$

solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results $M_1', M_2', \ldots M_k'$, and

combining said results of said sub-tasks to produce said receive message word M', wherein $M' = M$.

122. (New) A digital signature system, comprising:

a communication medium;

digital signature generating means coupled to said communication medium and adapted for transforming a message word M to a signed ciphertext word C and for transmitting said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$0 \le M \le n-1$, wherein n is a composite number of the form

$n=p_1 \bullet p_2 \bullet \ldots \bullet p_k$,

wherein k is an integer greater than 2 and p_1, p_2, ..., p_k are distinct random prime numbers, and wherein said signed ciphertext word C corresponds to a number representative of a signed form of said message word M and corresponds to

$C \equiv M^d \pmod{n}$,

wherein d is defined by

$d \equiv e^{-1} \bmod((p_1-1) \bullet (p_2-1) \bullet \ldots \bullet (p_k-1))$, and

e is a number relatively prime to (p_1-1), (P_2-1), ..., and (p_k-1); and

digital signature verification means communicatively coupled with said communication medium for receiving said signed ciphertext word C via said medium, and being operative to verify said signed ciphertext word C by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$e_1 \equiv e(\bmod(p_1-1)),$$

$$e_2 \equiv e(\bmod(p_2-1)), \text{ and}$$

$$\vdots$$

$$e_k \equiv e(\bmod(p_k-1)),$$

solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem to determine results $M_1', M_2', \ldots M_k'$, and

combining said results of said sub-tasks to produce said receive message word M', wherein $M' = M$.